

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18.

**(c) Study and report on computer crimes**

Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18.

**(d) Emergency disclosure exception**

**(1) Omitted**

**(2) Reporting of disclosures**

A government entity that receives a disclosure under section 2702(b) of title 18 shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after November 25, 2002.

(Pub. L. 107-296, title XXII, § 2207, formerly title II, § 225, Nov. 25, 2002, 116 Stat. 2156; renumbered title XXII, § 2207, Pub. L. 115-278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

**Editorial Notes**

**CODIFICATION**

Section was formerly classified to section 145 of this title prior to renumbering by Pub. L. 115-278.

Section is comprised of section 2207 of Pub. L. 107-296. Subsecs. (d)(1) and (e) to (j) of section 2207 of Pub. L. 107-296 amended sections 1030, 2511, 2512, 2520, 2701 to 2703, and 3125 of Title 18, Crimes and Criminal Procedure.

**§ 658. Cybersecurity recruitment and retention**

**(a) Definitions**

In this section:

**(1) Appropriate committees of Congress**

The term “appropriate committees of Congress” means the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

**(2) Collective bargaining agreement**

The term “collective bargaining agreement” has the meaning given that term in section 7103(a)(8) of title 5.

**(3) Excepted service**

The term “excepted service” has the meaning given that term in section 2103 of title 5.

**(4) Preference eligible**

The term “preference eligible” has the meaning given that term in section 2108 of title 5.

**(5) Qualified position**

The term “qualified position” means a position, designated by the Secretary for the purpose of this section, in which the incumbent performs, manages, or supervises functions that execute the responsibilities of the Department relating to cybersecurity.

**(6) Senior Executive Service**

The term “Senior Executive Service” has the meaning given that term in section 2101a of title 5.

**(b) General authority**

**(1) Establish positions, appoint personnel, and fix rates of pay**

**(A) General authority**

The Secretary may—

(i) establish, as positions in the excepted service, such qualified positions in the Department as the Secretary determines necessary to carry out the responsibilities of the Department relating to cybersecurity, including positions formerly identified as—

(I) senior level positions designated under section 5376 of title 5; and

(II) positions in the Senior Executive Service;

(ii) appoint an individual to a qualified position (after taking into consideration the availability of preference eligibles for appointment to the position); and

(iii) subject to the requirements of paragraphs (2) and (3), fix the compensation of an individual for service in a qualified position.

**(B) Construction with other laws**

The authority of the Secretary under this subsection applies without regard to the provisions of any other law relating to the appointment, number, classification, or compensation of employees.

**(2) Basic pay****(A) Authority to fix rates of basic pay**

In accordance with this section, the Secretary shall fix the rates of basic pay for any qualified position established under paragraph (1) in relation to the rates of pay provided for employees in comparable positions in the Department of Defense and subject to the same limitations on maximum rates of pay established for such employees by law or regulation.

**(B) Prevailing rate systems**

The Secretary may, consistent with section 5341 of title 5, adopt such provisions of that title as provide for prevailing rate systems of basic pay and may apply those provisions to qualified positions for employees in or under which the Department may employ individuals described by section 5342(a)(2)(A) of that title.

**(3) Additional compensation, incentives, and allowances****(A) Additional compensation based on title 5 authorities**

The Secretary may provide employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5.

**(B) Allowances in nonforeign areas**

An employee in a qualified position whose rate of basic pay is fixed under paragraph (2)(A) shall be eligible for an allowance under section 5941 of title 5, on the same basis and to the same extent as if the employee was an employee covered by such section 5941, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

**(4) Plan for execution of authorities**

Not later than 120 days after December 18, 2014, the Secretary shall submit a report to the appropriate committees of Congress with a plan for the use of the authorities provided under this subsection.

**(5) Collective bargaining agreements**

Nothing in paragraph (1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an office, component, subcomponent, or equivalent of the Department that is a successor to an office, component, subcomponent, or equivalent of the Department covered by the agreement before the succession.

**(6) Required regulations**

The Secretary, in coordination with the Director of the Office of Personnel Management, shall prescribe regulations for the administration of this section.

**(c) Annual report**

Not later than 1 year after December 18, 2014, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—

(1) discusses the process used by the Secretary in accepting applications, assessing candidates, ensuring adherence to veterans' preference, and selecting applicants for vacancies to be filled by an individual for a qualified position;

(2) describes—

(A) how the Secretary plans to fulfill the critical need of the Department to recruit and retain employees in qualified positions;

(B) the measures that will be used to measure progress; and

(C) any actions taken during the reporting period to fulfill such critical need;

(3) discusses how the planning and actions taken under paragraph (2) are integrated into the strategic workforce planning of the Department;

(4) provides metrics on actions occurring during the reporting period, including—

(A) the number of employees in qualified positions hired by occupation and grade and level or pay band;

(B) the placement of employees in qualified positions by directorate and office within the Department;

(C) the total number of veterans hired;

(D) the number of separations of employees in qualified positions by occupation and grade and level or pay band;

(E) the number of retirements of employees in qualified positions by occupation and grade and level or pay band; and

(F) the number and amounts of recruitment, relocation, and retention incentives paid to employees in qualified positions by occupation and grade and level or pay band; and

(5) describes the training provided to supervisors of employees in qualified positions at the Department on the use of the new authorities.

**(d) Three-year probationary period**

The probationary period for all employees hired under the authority established in this section shall be 3 years.

**(e) Incumbents of existing competitive service positions****(1) In general**

An individual serving in a position on December 18, 2014, that is selected to be converted to a position in the excepted service under this section shall have the right to refuse such conversion.

**(2) Subsequent conversion**

After the date on which an individual who refuses a conversion under paragraph (1) stops serving in the position selected to be converted, the position may be converted to a position in the excepted service.

**(f) Study and report**

Not later than 120 days after December 18, 2014, the National Protection and Programs Directorate shall submit a report regarding the availability of, and benefits (including cost savings and security) of using, cybersecurity personnel and facilities outside of the National

Capital Region (as defined in section 2674 of title 10) to serve the Federal and national need to—

(1) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Subcommittee on Homeland Security of the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives.

(Pub. L. 107-296, title XXII, § 2208, formerly title II, § 226, as added Pub. L. 113-277, § 3(a), Dec. 18, 2014, 128 Stat. 3005; renumbered title XXII, § 2208, Pub. L. 115-278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178.)

#### Editorial Notes

##### CODIFICATION

Section was formerly classified to section 147 of this title prior to renumbering by Pub. L. 115-278.

#### Statutory Notes and Related Subsidiaries

##### CHANGE OF NAME

Reference to National Protection and Programs Directorate of the Department of Homeland Security deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department, see section 652(a)(2) of this title, enacted Nov. 16, 2018.

### § 659. National cybersecurity and communications integration center

#### (a) Definition

The term “cybersecurity vulnerability” has the meaning given the term “security vulnerability” in section 650 of this title.

#### (b) Center

There is in the Department a national cybersecurity and communications integration center (referred to in this section as the “Center”) to carry out certain responsibilities of the Director. The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Executive Assistant Director for Cybersecurity.

#### (c) Functions

The cybersecurity functions of the Center shall include—

(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities, including the implementation of title I of the Cybersecurity Act of 2015 [6 U.S.C. 1501 et seq.];

(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

(3) coordinating the sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents across the Federal Government;

(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, in-

cluding cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cyber threat indicators, defensive measures, cybersecurity risks, and incidents;

(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n), as appropriate; and

(C) sharing the analysis conducted under subparagraph (A) and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B), as appropriate, with Federal and non-Federal entities;

(6) upon request, providing operational and timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation, which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions;

(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

(A) facilitate information security;

(B) strengthen information systems against cybersecurity risks and incidents; and

(C) share cyber threat indicators and defensive measures;

(8) engaging with international partners, in consultation with other appropriate agencies, to—

(A) collaborate on cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents; and

(B) enhance the security and resilience of global cybersecurity;

(9) sharing cyber threat indicators, defensive measures, mitigation protocols to counter cybersecurity vulnerabilities, as appropriate, and other information related to cybersecurity risks and incidents with Federal and non-Federal entities, including across sectors of critical infrastructure and with State and major urban area fusion centers, as appropriate;

(10) participating, as appropriate, in national exercises run by the Department;

(11) in coordination with the Emergency Communications Division of the Department, assessing and evaluating consequence, vulnerability, and threat information regarding cyber incidents to public safety communications to help facilitate continuous improvements to the security and resiliency of such communications;

(12) detecting, identifying, and receiving information for a cybersecurity purpose about security vulnerabilities relating to critical infrastructure in information systems and devices; and

(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as de-